EXHIBIT 2

AO 88B (Rev. 02/14) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of Georgia

Donna Curling, et al.
Plaintiff
v.
Brad Raffensperger, et al.
Defendant

Civil Action No. 1:17-cv-02989-AT

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To:

Cathleen A. Latham

(Name of person to whom this subpoena is directed)

☑ *Production:* **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material:

See Attachment A.

Place:	Date and Time:
Office of Kathryn Grant 202 W. Gordon St., Unit E Valdosta, GA 31602	07/26/2022 05:00 pm

☐ *Inspection of Premises:* **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 07/19/2022

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* Coalition for Good Governance, , who issues or requests this subpoena, are:

Bruce P. Brown, 1123 Zonolite Rd. NE St. 6, Atlanta GA 30306 bbrown@brucepbrownlaw.com (404) 386-6856

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 1:17-cv-02989-AT

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____

on *(date)* _____ .

☐ I served the subpoena by delivering a copy to the named person as follows: _____

_____

_____ on *(date)* _____ ; or

☐ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

EXHIBIT A

ATTACHMENT A: DOCUMENTS DESIGNATED FOR PRODUCTION

Notice to Nonparty:

Please produce responsive documents by the date provided in the accompanying subpoena.

Definitions

The following words, terms, or phrases shall, for purposes of the requests for production of documents below, have the meanings specified, unless otherwise expressly stated in each request:

"Access to Coffee County's Election System, EMS Servers and Election Data" means any activity that took place after November 3, 2020, in which Persons other than Coffee County's Election Superintendent, full time employees of the Superintendent, employees of the Georgia Secretary of State, or representatives of Dominion Voting System, were present in the room containing Coffee County's EMS server, or had physical access to components of the Coffee County Election System except in conjunction with the official conduct of polling place voting.

"All" and "each" shall be construed as all and each.

"And" as well as "or" are to be construed either disjunctively or conjunctively as necessary to bring within the scope of the Requests all documents or other information that might otherwise be construed to be outside their scope.

"Any" means each and every.

"Communication" means any transmission of information by any means, including without limitation: (a) any written letter, memorandum, or other Document of any kind by mail, courier, other delivery services, telecopy, facsimile, telegraph, electronic mail, electronic text messages, voicemail, or any other means; (b) any telephone call, or video call, whether or not such call was by chance or prearranged, formal or informal; and (c) any conversation or meeting between two or more Persons, whether or not such contact was by chance or prearranged, formal or informal.

"Concerning," "related to" or "relating to," and "regarding" mean analyzing, alluding to, concerning, considering, commenting on, consulting, comprising, containing, contradicting, describing, dealing with, discussing, establishing, evidencing, identifying, involving, noting, recording, reporting on, related to, relating to, reflecting, referring to, regarding, stating, showing, studying, mentioning, memorializing, or pertaining to, in whole or in part.

"Document" and "documents" shall be construed as synonymous in meaning and equal in scope to the usage of that term in Rule 34(a), and includes "tangible things" (as that term is used in Rule 34(a)(1)(b)) as well as anything that falls within the definition or meaning of "electronically stored information" (as that

term is used in Rule 34(a)(1)(A)) or of "writings" or "recordings" in Federal Rule of Evidence 1001. A draft or non-identical copy of a document shall be considered a separate document within the meaning of the term "document," as used in the Requests.

"Election System" means any servers, desktops, laptops, tablets, smart phones, removable media (such as memory cards), ballot-marking devices (BMDs) (including ImageCastX Ballot-Marking Devices), BMD-adjacent equipment (including ImageCast Precinct Polling Place Scanner and associated printers or touchscreens), ImageCast Central Count Scanner ("ICC") and any software and firmware installed on any such scanners, servers, devices, BMDs, or BMD-adjacent equipment (such as any version of the Election Management System (EMS), PollPads, or the software associated with the "Dominion Voting Democracy Suite" (D-Suite) and KnowInk PollPads) used to check in voters, activate BMDs, record, tabulate, or secure votes in any election in the state of Georgia.

"Including" means including without limitation.

"Person" means and includes a natural person (i.e., an individual), a group of natural persons acting as individuals, a group of individuals acting in a collegial or concerted capacity (e.g., as a committee, a board of directors or advisors, etc.), an

association, firm, corporation, joint venture, partnership, company, governmental unit or agency, and any other business, enterprise, or entity, unless otherwise limited or specified in the Requests.

"Secretary of State" means Secretary of State Brad Raffensperger, the Office of the Georgia Secretary of State, as well as the respective agents, employees, representatives, consultants, counsel, and anyone else acting on behalf of each or all of the forgoing. This may be abbreviated as "SOS."

"Superintendent:" means the Coffee County Board of Elections and Registration of Coffee County, Georgia.

"Relevant Time Period" means July 1, 2020, until the present unless otherwise indicated.

"You" or "Your" mean Cathy Latham and any other person acting on Your behalf or under Your direction or control with respect to the subject matter of the Requests.

Instructions

1. For each request, you are to produce entire documents including all attachments, enclosures, cover letters, memoranda, exhibits, and appendices. Copies that differ in any respect from an original (because, by way of example only, handwritten or printed notations have been added) shall be treated as separate

documents and produced separately. Each draft of a document is a separate document. A request for a document shall be deemed to include a request for any and all transmittal sheets, cover letters, exhibits, enclosures, or attachments to the document, in addition to the document itself. These document requests shall not be deemed to call for identical copies of documents. "Identical" means precisely the same in all respects; for example, a document with handwritten notes or editing marks shall not be deemed identical to one without such notes or marks.

2. Provide all electronically stored information ("ESI") in standard, single-page Group IV TIFF format with searchable text and metadata in a Relativity or similar load file. Also, provide any spreadsheet or presentation files, including Microsoft Access, Excel, and PowerPoint files, as well as audio, audiovisual, and video files, in their native formats. Also, provide any responsive Election System files including but not limited to software installation files, configuration files, input files, intermediate data files, output files, report files, system and application log files, or other election software or data files (in their native formats) associated with any component of the Dominion voting system as used in Georgia elections (the Democracy Suite election management system applications, ImageCast Precinct and ImageCast Central tabulators, and ImageCast X BMDs, and associated peripherals (including KnowInk PollPads and related

software)), including but not limited to software and/or firmware installation files (such as MSI, EXE, or APK or files in a proprietary binary format); scripts and/or configuration files used to provision or harden the installed software or firmware; EMS election project files, election project backup files, compressed archives of election project databases, and system permission rule sets; Microsoft SQL Database files; election definition and behavioral and configuration files used by PollPads, ICX, ICP, and ICC devices (DAT files for ICX BMDs and files in the binary file formats used by the ICP and ICC tabulators); security credentials and encryption keys, including authentication data used to program security cards and keys to be used by the ICX, ICP, and ICC devices; result files (in the proprietary binary file format collected from the ICP and ICC tabulators); scanned ballot images; result reports in XML, PDF, HTML, and Excel formats; and device log, system log, and audit log files and reports. Produce the metadata for any responsive ESI with the responsive data, including the following fields: custodian(s), author(s), recipient(s), copy recipient(s), blind copy recipient(s), company name, subject, file sent date/time, file received date/time, file creation date/time, file modification date/time, file access date/time, time zone, beginning bates, ending bates, page count, family bates range, hash value, application type,

file type, file name, file size, file path, and folder path. Documents produced in native format shall be accompanied by a native link field.

3. Provide all hard copy documents as image files with searchable OCR text and unitize the hard copy documents to the extent possible (i.e., multi-page documents shall be produced as a single document and not as several single-page documents). Hard copy documents shall be produced as they are kept in the usual course, reflecting attachment relationships between documents and information about the file folders within which the document is found.

4. If you withhold or intend to withhold any documents or other information requested by the Requests on the ground of the attorney-client privilege, work-product doctrine, or other privilege, doctrine, or immunity, please provide a privilege log that meets the requirements of Rule 26(b)(5), including: (a) the document or information alleged to be so protected from production by author, subject matter, date, number of pages, attachments, and appendices; (b) the names and job titles of all recipients of the information or document, including any "blind copy" recipients and any person to whom the information or document was distributed, shown, or explained; (c) the document's current custodian(s); and (d) all bases, factual and legal, upon which the claim of protection from discovery rests.

5. If only a portion of a responsive document or other requested information is claimed to be privileged against production, you should produce the responsive non-privileged portion of the document or other information in redacted form, provided that the redacted material is identified and the basis for the claim of privilege or protection is stated as provided in Instruction No. 4 above.

6. If you contend that any of the categories of the Requests are objectionable in whole or in part, please state with particularity each objection, the basis for it, and the categories of the Requests to which the objection applies, and otherwise fully respond to the category insofar as it is not deemed objectionable.

7. The documents responsive to these requests are to be produced as they were kept in the ordinary course of business, or in the way they were produced or otherwise provided to you from a third party, and, if the documents were produced by a third party, the identity of the third party shall be apparent or provided.

8. If any document responsive to this request was, but no longer is in your possession, state whether it is missing or lost; if it has been destroyed; if it has been transferred, voluntarily or involuntarily, to others; or if it has otherwise been disposed of. In each instance, identify the document fully, explain the circumstances, and identify the people having knowledge of such circumstances.

9. If you contend that any documents covered in these requests are not reasonably accessible or would be unduly burdensome to locate or produce, identify such documents by category and source and provide detailed information regarding the burden or cost you claim is associated with the search for or production of such documents.

10. Unless clearly indicated otherwise: (a) the use of a verb in any tense shall be construed as the use of that verb in all other tenses; (b) the use of the feminine, masculine, or neuter genders shall include all genders; and (c) the singular form of a word shall include the plural and vice versa.

11. The Requests are deemed to be continuing so as to require the timely submission of supplemental responses and the production of additional documents or other information pursuant to the Rules and other applicable authority. Plaintiffs specifically reserve the right to seek supplemental responses and additional supplemental production of documents before trial.

12. Documents shall be produced to Plaintiffs via e-mail or comparable electronic means to their counsel of record or other individuals identified by Plaintiffs for receipt.

Document Requests

1. Documents that evidence, refer to, or reflect approximately when any Access to Coffee County's Election System, EMS Servers and Election Data took place or was requested.

2. Documents that evidence, refer to, or reflect the Persons involved in any way, or who have knowledge of, any Access to Coffee County's Election System, EMS Servers and Election Data, including, but not limited to, Persons who approved, financed, requested, organized, planned, communicated about, led, participated in, were present in Coffee County's Election Office during, or have knowledge of such events.

3. Documents that evidence, refer to, or reflect what data, ballots, components, systems, and processes were accessed, reviewed, or requested during any Access to Coffee County's Election System and EMS Servers.

4. Documents that evidence, refer to, or reflect how any Person was able to gain access to or review Coffee County's Election System and EMS servers and election records during any Access to Coffee County's Election System, EMS Servers and Election Data, including requests for access approved by official or the Coffee County Superintendent.

5. Documents that evidence, refer to, or reflect which Coffee County Election System images, devices, or documents were reviewed, scanned and/or imaged and/or copied by any Person as part of any Access to Coffee County's Election System, EMS Servers and Election Data.

6. All electronic files, including but not limited to election data, server images, images of equipment internal memory, removable media, ballot scans or ballot images obtained during any Access to Coffee County's Election System, EMS Servers and Election Data by You or other Persons.

7. Documents showing Your involvement in, knowledge of, or observation of any planned or actual Access to Coffee County's Election System, EMS Servers and Election Data.

8. All Documents that evidence, refer to, or reflect any Communications (oral, electronic or written) by or between You and the Secretary of State, the State Elections Board and its members, Coffee County officials and employees, other Georgia counties' official, or other third parties relating to any Access to Coffee County's Election System, EMS Servers and Election Data, including any Communications concerning the images or electronic files accessed, reviewed or obtained during any Access to Coffee County's Election System, EMS Servers and Election Data.

9. All Documents that evidence, refer to, or reflect any actual or potential security vulnerabilities, risks, failings, deficiencies, concerns, complaints, hacks, tabulation discrepancies, or compromises involving any aspect of Coffee County's Election System, including but not limited to any computer systems or network environments that support the operation of the Election System, and including the errors and discrepancies experienced in the November 2020 machine recount.

10. All Documents or Communications that support or are related to the testimony that You gave to the Election Law Study Subcommittee of the Senate Judiciary Committee on December 30, 2020, including all Communications with the Secretary of State described in or regarding Your testimony.

11. All Documents, including Communications, that relate to your status as a "whistleblower," as stated by Preston Haliburton and recorded on page 3 of the Minutes of the Election Law Study Subcommittee of the Standing Senate Judiciary Committee which can be found at http://www.senatorligon.com/MINUTES_2nd%20Hearing%2030_Dec_2020.pdf.

12. All Documents that evidence, refer to, or reflect any Communications by or between You (internal communications), the Secretary of State, the State Elections Board and its members, other Georgia counties' officials, or other third

parties, regarding this litigation, or any government agency investigation of Coffee County Georgia election-related matters

13. All Documents that evidence, refer to, or reflect any copying of, imaging of, review of, or access to, voted ballots or any component of Georgia's Election System, or any data located on any such component, that was not duly authorized by one or more State election officials with authority to lawfully allow such access.

14. All documents that evidence, refer to, or reflect any Communications between You and Misty Hampton, Jil Ridlehoover, Scott Hall, Eric Chaney, Matthew McCullough, Paul Maggio, Jeffrey Lenberg, Russell Ramsland, Ben Cotton, Doug Logan, Greg Freemeyer, Conan Hayes, David Shafer, Anthony Rowell, Shawn Still, or Patrick Byrne related or referring to any Person planning to visit Coffee County, Georgia for the purpose of reviewing or obtaining November 2020 electronic election records.

15. All Documents that evidence, refer to, or reflect any Communications between You and Scott Hall, Patrick Byrne, Eric Chaney, Misty Hampton, Jil Ridlehoover, Matthew McCullough, Anthony Rowell, Rudy Giuliani, Jenna Ellis, Alex Cruce, Garland Favorito, Robert Cheeley, Lin Wood, Doug Logan, Sidney Powell, Russell Ramsland, Mark Cook, Paul Maggio, Greg Freemeyer, Conan

Hayes, Phil Waldron, Michael Flynn, Jeffrey Lenberg, Ben Cotton, Shawn Still, Kevin Moncla, David Shafer, any member of the Georgia General Assembly serving during 2020, and/or other third parties concerning the potential imaging or copying of any Georgia EMS server, or forensic auditing using such server records, or this litigation.

16. All Documents that evidence, refer to, or reflect Communications between You and any Person regarding the names of files or data desired to be obtained for forensic analysis of Election System components or electronic data stored on the Election System used in Georgia's November 2020 election.

17. All Documents, including Communications, that evidence names of any passengers or invited passengers for a flight on a private aircraft from Atlanta, Georgia to Coffee County, Georgia on January 7, 2021.

18. All Documents, including Communications, that evidence, refer to or relate to Coffee County's November 2020 election's electronic Cast Vote Record files.

19. All Documents, including Communications, that evidence financial transactions, expense reimbursements, financial compensation, with respect to or related to Your activities or any Person's activities related to reviewing or auditing Georgia's Election System components or 2020 election records.

20. All Documents, including Communications with any Person, that evidence the basis or support for, or potential of, the mention of Coffee County in either of the Draft Executive Orders attached at Exhibit 1.

EXHIBIT

1

December 16, 2020

PRESIDENTIAL FINDINGS
TO PRESERVE COLLECT AND ANALYIZE NATIONAL SECURITY INFORMATION
REGARDING THE 2020 GENERAL ELECTION

By the authority vested in me as President of the United States pursuant to the Constitution and laws of the United States of America, including Article 2 section 1 of the U.S. Constitution, Executive Orders 12333, 13848, National Security Presidential Memoranda 13 and 21, the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA) and all applicable Executive Orders derived therefrom, the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code:

I, Donald J. Trump, President of the United States, find that the forensic report of the Antrim County, Michigan voting machines, released December 13, 2020, and other evidence submitted to me in support of this order, provide probable cause sufficient to require action under the authorities cited above because of evidence of international and foreign interference in the November 3, 2020, election. Dominion Voting Systems and related companies are owned or heavily controlled and influenced by foreign agents, countries, and interests. The forensic report prepared by experts found that "the Dominion Voting System is intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results. The system intentionally generates an enormously high number of ballot errors... The intentional errors lead to bulk adjudication of ballots with no oversight, no transparency, and no audit trail. This leads to voter or election fraud." The report found the election management system to be wrought with unacceptable and unlawful vulnerabilities—including access to the internet— probable cause to find evidence of fraud, and numerous malicious actions.

There is also probable cause to find that Dominion Voting Systems, Smartmatic, Electronic Systems & Software, and Hart Inter Civic, Clarity Election Night Reporting, Edison Research, Sequoia, Scytl, and similar or related entities, agents or assigns, have the same flaws and were subject to foreign interference in the 2020 election in the United States. There is probable cause to find these systems bear the same crucial code "features" and defects that allowed the same outside and foreign interference in our election, in which there is probable cause to find votes were in fact altered and manipulated contrary to the will of the voters.

Dominion Voting Systems is based in Toronto, Canada, and assigns its intellectual property including patents on its firmware and software to Hong Kong and Shanghai Bank Corporation (HSBC), a bank with its foundation in China and its current headquarters in London, United Kingdom. The Dominion Voting system is owned and controlled by foreign entities. Multiple expert witnesses and cyber experts identified acts of foreign interference in the election prior to November 3, 2020 and continued in the following weeks. In fact, there is probable cause to find a massive cyber-attack by foreign interests on our crucial national infrastructure surrounding our election—not the least of which was the hacking of the voter registration system by Iran. (E.O. 13800 of May 11, 2017)

Just **days prior to the election** of November 3, 2020, federal Judge Totenberg found, after three days of testimony including by Dominion executive Eric Coomers:

> There are "true risks posed by the new BMD [Ballot Marking Device of Georgia's Dominion Voting Systems] voting system as well as its manner of implementation. These risks are neither hypothetical nor remote under the current circumstances. The insularity of the Defendants' and Dominion's stance here in evaluation and management of the security and vulnerability of the BMD system does not benefit the public or citizens' confident exercise of the franchise. The stealth vote alteration or operational interference risks posed by malware that can be effectively invisible to detection, whether intentionally seeded or not, are high once implanted, if equipment and software systems are not properly protected, implemented, and audited. The modality of the BMD systems' capacity to deprive voters of their cast votes without burden, long wait times, and insecurity regarding how their votes are actually cast and recorded in the unverified QR code makes the potential constitutional deprivation less transparently visible as well, at least until any portions of the system implode because of system breach, breakdown, or crashes. Any operational shortcuts now in setting up or running election equipment or software creates other risks that can adversely impact the voting process.
>
> "The Plaintiffs' national cybersecurity experts convincingly present evidence that this is not a question of "might this actually ever happen?" – but "when it will happen," especially if further protective measures are not taken. Given the masking nature of malware and the current systems described here, if the State and Dominion simply stand by and say, "we have never seen it," the future does not bode well.
>
> "Still, this is year one for Georgia in implementation of this new BMD system as the first state in the nation to embrace statewide implementation of this QR barcode-based BMD system for its entire population. Electoral dysfunction – cyber or otherwise – should not be desired as a mode of proof. It may well land unfortunately on the State's doorstep. The Court certainly hopes not."[1]

And, yet it did. Every defect and hazard of which Judge Totenberg warned happened in Georgia. Witnesses in Georgia have provided evidence of crashes, the replacement of a server, impermissible updates to the system, connections to the internet, and both Coffee and Ware counties have identified a significant percentage of votes being wrongly allocated contrary to the will of the voter. Coffee County Georgia has refused to certify its result.

Accordingly, I hereby order:

(1) Effective immediately, the Secretary of Defense shall seize, collect, retain and analyze all machines, equipment, electronically stored information, and material records required for retention under United States Code Title 42, Sections 1974-1974(e), including but not limited to those identified in footnote 1. The Secretary of Defense has discretion to determine the

---

[1] Case 1:17-cv-02989-AT Document 964 Filed 10/11/20 Page 146 of 147

interdiction of national critical infrastructure supporting federal elections. Designated locations will be identified in the operation order.

(2) Within 7 days of commencement of operations, the initial assessment must be provided to the Office of the Director of National Intelligence. The final assessment must be provided to the Office of the Director of National Intelligence no later than 60 days from commencement of operations.

(3) The Director of National Intelligence shall deliver this assessment and appropriate supporting information to the President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, and the Secretary of Homeland Security.

(4) A direct liaison to be authorized to coordinate as required between the applicable U.S. Departments and Agencies.

(5) The Secretary of Defense may select by name or by unit federalization of appropriate National Guard support.

(6) The Assistant Secretary of Defense for Homeland Security will coordinate support requirements as needed from the Department of Homeland Security.

(7) The appointment of a Special Prosecutor to oversee this operation and institute all criminal and civil proceedings as appropriate based on the evidence collected and provided all resources necessary to carry out her duties consistent with federal laws and the Constitution.

December 17, 2020

PRESIDENTIAL FINDINGS
TO SEIZE, COLLECT, PRESERVE AND ANALYZE NATIONAL SECURITY INFORMATION REGARDING THE 2020 GENERAL ELECTION

By the authority vested in me as President of the United States pursuant to the Constitution and laws of the United States of America, including Article 2 section 1 of the U.S. Constitution, Executive Orders 12333, 13848, National Security Presidential Memoranda 13 and 21, the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA) and all applicable Executive Orders derived therefrom, the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and Section 301 of Title 3, United States Code:

I, Donald J. Trump, President of the United States, find that the forensic report of the Antrim County, Michigan voting machines, released December 13, 2020, and other evidence and sworn testimony submitted to me in support of this order, provide probable cause sufficient to require action under the authorities cited above because of evidence of foreign interference and widespread fraud leading up to and including the November 3, 2020 election. Dominion Voting Systems and related companies are owned or heavily controlled and influenced by foreign agents, countries, and interests. The forensic report prepared by experts found that "the Dominion Voting System is intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results. The system intentionally generates an enormously high number of ballot errors... The intentional errors lead to bulk adjudication of ballots with no oversight, no transparency, and no audit trail. This leads to voter or election fraud." The report found the election management system to be wrought with unacceptable and unlawful vulnerabilities—including access to the internet— probable cause to find evidence of fraud, and numerous malicious actions.

There is also probable cause to find that Dominion Voting Systems, Smartmatic, Electronic Systems & Software, and Hart Inter Civic, Clarity Election Night Reporting, Edison Research, Sequoia, Scytl, Election Source and similar or related entities, agents or assigns, have the same flaws and were subject and vulnerable to foreign interference in the 2020 election in the United States. There is probable cause to find these systems bear the same crucial code "features" and defects that allowed the same outside and foreign interference in our election, in which there is probable cause to find votes were in fact altered and manipulated contrary to the will of the voters.

Dominion Voting Systems is based in Toronto, Canada, and assigns its intellectual property including patents on its firmware and software to Hong Kong and Shanghai Bank Corporation (HSBC), a bank with its foundation in China and its current headquarters in London, United Kingdom. The Dominion Voting system is owned and controlled by foreign entities. Multiple expert witnesses and cyber experts identified acts of foreign interference in the election prior to November 3, 2020 and continued in the following weeks. In fact, there is probable cause to find a massive cyber-attack by foreign interests on our crucial national infrastructure surrounding our election—not the least of which was the hacking of the voter registration system by Iran. (E.O. 13800 of May 11, 2017).

Just **days prior to the election** of November 3, 2020, federal Judge Totenberg found, after three days of testimony including by Dominion executive Eric Coomers:

> There are "true risks posed by the new BMD [Ballot Marking Device of Georgia's Dominion Voting Systems] voting system as well as its manner of implementation. These risks are neither hypothetical nor remote under the current circumstances. The insularity of the Defendants' and Dominion's stance here in evaluation and management of the security and vulnerability of the BMD system does not benefit the public or citizens' confident exercise of the franchise. The stealth vote alteration or operational interference risks posed by malware that can be effectively invisible to detection, whether intentionally seeded or not, are high once implanted, if equipment and software systems are not properly protected, implemented, and audited. The modality of the BMD systems' capacity to deprive voters of their cast votes without burden, long wait times, and insecurity regarding how their votes are actually cast and recorded in the unverified QR code makes the potential constitutional deprivation less transparently visible as well, at least until any portions of the system implode because of system breach, breakdown, or crashes. Any operational shortcuts now in setting up or running election equipment or software creates other risks that can adversely impact the voting process.
>
> "The Plaintiffs' national cybersecurity experts convincingly present evidence that this is not a question of "might this actually ever happen?" – but "when it will happen," especially if further protective measures are not taken. Given the masking nature of malware and the current systems described here, if the State and Dominion simply stand by and say, "we have never seen it," the future does not bode well.
>
> "Still, this is year one for Georgia in implementation of this new BMD system as the first state in the nation to embrace statewide implementation of this QR barcode-based BMD system for its entire population. Electoral dysfunction – cyber or otherwise – should not be desired as a mode of proof. It may well land unfortunately on the State's doorstep. The Court certainly hopes not."[1]

And, yet it did. Every defect and hazard of which Judge Totenberg warned happened in Georgia. Witnesses in Georgia have provided evidence of crashes, the replacement of a server, impermissible updates to the system, connections to the internet, and both Coffee and Ware counties have identified a significant percentage of votes being wrongly allocated contrary to the will of the voter. Coffee County Georgia has refused to certify its result.

Further foreign intelligence service involvement in the 2020 elections is evidenced by the involvement of Kavtech, a Pakistan based Business Intelligence firm with ties to the ISI (Pakistani Inter-Service Intelligence Agency), that directly received e-mails from the Nevada Secretary of State containing personally identifiable voter registration information. It is unknown how this information may have been exploited. (see attachment).

---

[1] Case 1:17-cv-02989-AT Document 964 Filed 10/11/20 Page 146 of 147

Accordingly, I hereby order:

(1) Effective immediately, the Secretary of Homeland Security shall seize, collect, preserve, protect, retain and analyze all machines, equipment, electronically stored information, and material records required for retention under United States Code Title 42, Sections 1974-1974(e), including but not limited to those identified in footnote 1. The Secretary of Homeland Security has discretion to determine the interdiction of federal and state critical infrastructure that supported the federal elections of 2020, including hardware, software, documentation, ballots, key cards and any other physical items to include security badges, polling official rosters, and related items. Designated locations will be identified in the operation order.

(2) The Secretary of Homeland Security and all of the Secretary's agents and assigns shall have the power to immediately seek the issuance of any and all search warrants and other warrants or legal powers as may be necessary to carry out and execute this directive.

(3) Within 7 days of commencement of operations, the initial assessment of information and physical items seized in the above order must be provided to the Office of the Director of National Intelligence. The final assessment must be provided to the Office of the Director of National Intelligence no later than 60 days from commencement of operations.

(4) In accordance with my Executive Order dated September 2018, the Director of National Intelligence shall deliver this assessment and appropriate supporting information to the President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense and the Attorney General.

(5) A direct liaison is authorized to coordinate as required between the applicable U.S. Departments and Agencies. Director, National Intelligence shall ensure access to classified information is made available to those with appropriate clearances. Director, National Intelligence is authorized to provide additional compartmented "read on" where applicable. These special category indoctrinations will be limited in scope with focus on foreign influence in national elections.

(6) The Secretary of Homeland Security shall request the Secretary of Defense to provide select personnel/capabilities by name or by unit (federalization of appropriate National Guard assets authorized) in support of a Defense Support to Civil Authorities (DSCA) mission.

(7) The Assistant Secretary of Defense for Homeland Security shall coordinate support requirements as needed from the Department of Defense.

(8) The appointment of a Special Prosecutor to oversee this operation and institute all criminal and civil proceedings as appropriate based on the evidence collected and provided all resources necessary to carry out her duties consistent with federal laws and the Constitution.